CLAIMS

1. A method for authenticating and protecting data, comprising the providing of a plurality of challenging mines dispersed within an executable program file, each mine being dependent on one validation key located in at least one other mine, and optionally on additional keys, for allowing proper use of the executable program file and content files that can be activated by said executable program file.

2. A method according to claim 1, wherein the additional keys comprise:
   - a signature key stored on a media and accessible by standard devices for read-only;
   - a content key stored on the media of the content files; and
   - an authentication key stored in some type of media remote from the one in use.

3. A method according to claim 1, wherein the mines are concealed within the executable program file.

4. A method according to claim 3, wherein the mines are concealed within the executable program file by means of being encrypted.

5. A method according to claim 1, wherein a portion of the executable program file is encrypted within the location of a mine.

6. A method according to claim 1, wherein the mines are encrypted.

7. A method according to claim 5, wherein the proper operation/use of said portion of executable program file is possible only when properly decrypting it using a validation, authentication, or signature key, or a combination thereof, as a decrypting key.

8. A method according to claim 1, wherein the mines are encrypted using a validation, authentication, or signature key, or a combination thereof.

9. A method according to claim 2, wherein the content files are encrypted by means of content keys.

10. A method according to claim 9, wherein the proper use of a content file protected by a mine is possible only when finding a corresponding content key for decrypting said file.

11. A method according to claim 2, wherein the proper use of the portion of the executable program file that is protected by a mine further depends on the existence of an authentication key on a medium of the provider of the software, accessible via the Internet.
12. A method according to claim 1, wherein the effecting of the mines within the executable program file involves two steps: designating and arming.
13. A method according to claim 12, wherein the designating and arming steps are carried out by two separate entities.
14. A method according to claim 13, wherein the designating step is carried out by the author/producer of the data.
15. A method according to claim 13, wherein the arming step is carried out by a data protecting professional.
16. A method according to claim 1, wherein the dependence between mines is carried out by means of relative addressing.
17. A method according to claim 1, wherein the content files are image, voice, video files, or any other digital file.